UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/422,431	10/12/1999	JOHN R. HIND	RSW9-99-113	5532

7590 12/23/2003

JEANINE S RAY YARLETTS
IBM CORP T81 BLDG 062
P O BOX 12195
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER	
TRAN, TONGOC	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/23/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/422,431	HIND ET AL.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 October 1999*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. This office action is in response to Applicants' application serial no. 09/422,431 filed on 10/21/1999.

Specification

2. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-12, 14-15, 19-33, 35-36, 40-44, 56-57 and 61-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. (U.S. Patent No. 6,585,778 hereinafter Hind) in view of Gennaro et al. (U.S. Patent No. 5,937,066 hereinafter Gennaro) and Schneck et al. (U.S. Patent No. 5,933,498).

In respect to claim 1, Hind discloses a computer program product embodied on computer readable media readable by a computing system in a computing environment, for enforcing security policy using style sheet processing, comprising:

an input document (see col. 4, lines 16-18);

one or more stored policy enforcement objects, wherein each of said stored policy enforcement objects specifies a security policy to be associated with zero or more elements of said input document (see col. 4, lines 1-4 and lines 11-32);

a Document Type Definition (DTD) corresponding to said input document, wherein said DTD has been augmented with one or more references to selected ones of said stored policy enforcement objects (see 4, lines 16-23);

an augmented style sheet processor, wherein said augmented processor further comprises:

computer-readable program code means for loading said DTD (see col. 4, lines 25);

computer-readable program code means for resolving each of said one or more references in said loaded DTD (see col. 4, lines 25-26);

computer-readable program code means for instantiating said policy enforcement objects associated with said resolved references (see col. 4, lines 26-28);

computer-readable program code means for executing selected ones of said instantiated policy enforcement objects during application of one or more style sheets to said input document, wherein a result of said computer-readable program code means for executing is an interim transient document reflecting said execution (see col. 4, lines 28-31);

Hind does not disclose but Gennaro discloses a computer-readable program code means for generating one or more random encryption keys; and computer-readable program code means for encrypting each of said one or more random

encryption keys (see col. 7, lines 52-67 and col. 8, lines 44-54). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the Hind's teaching of enforcing data policy using style sheet processing with security feature of using random encryption keys and encrypting the encryption key taught by Gennaro for better protecting transmitted document by avoiding the disadvantage of key sharing and to keep the encryption key safe by encrypting the encryption key (see Hind, col. 8, lines 44-45).

Furthermore, Hind does not disclose but Schneck discloses a computer-readable program code means for encrypting selected elements of said interim transient document, wherein a particular one of said generated random encryption keys may be used to encrypt one or more of said selected elements, while leaving zero or more other elements of said interim transient document unencrypted (see Fig. 1 and 2, col. 9, lines 38-59 and col. 10, lines 34-42). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Hind's teaching of enforcing data policy using style sheet processing with the partial encryption features taught by Schneck in order to enable the user to access the data in various controlled ways depending on access rules (see Schneck, col. 9, lines 55-59).

Hind does not disclose but Schneck discloses creating an encrypted output document comprising said zero or more unencrypted elements, said selected encrypted elements, and said encrypted encryption keys (see Fig. 2, 4 and 6, col. 12, lines 17-26 and col. 13, lines 36-50). Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Hind's teaching of enforcing

data policy using style sheet processing with packaged data that includes encrypted body part, unencrypted body and other encrypted information taught by Schneck for better tamper resistant of transmitted document.

Furthermore, Hind does not disclose but Gennaro computer-readable program code means for requesting said encrypted output document by a key recovery agent; computer-readable program code means for receiving said requested output document; and an augmented document processor, comprising (see col. 9, lines 5-24, col. 10, lines 1-27):

computer-readable program code means for decrypting each of said encrypted encryption keys (see col. 10, lines 22-24); and

computer-readable program code means for decrypting said requested output document using said decrypted keys, thereby creating a result document (see col. 10, lines 51-67). Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Hind's enforcing data policy using style sheet processing with Gennaro's key recovery system utilizing key recovery agent to recover encryption key to prevent the loss of keys that may result in loss of important stored data (see Gennaro, col. 2, lines 25-30).

In respect to claim 2, Hind, Gennaro and Schneck disclose the computer program product according to Claim 1, Hinder further comprising computer readable program code means for rendering said result document on said client device (see Hind, col. 7, lines 19-25).

In respect to claim 3, Hind, Gennaro and Schneck disclose the computer program product according to Claim 1, wherein said interim transient document comprises one or more encryption tags identifying elements needing encryption (see Schneck, col. 7, lines 37-39) .

In respect to claim 4, Hind, Gennaro and Schneck disclose the computer program product according to Claim 1, wherein said input document is specified in an Extensible Markup Language (XML) notation (see Hind, col. 7, lines 19-50).

In respect to claim 5, Hind, Gennaro and Schneck disclose the computer program product according to Claim 4, wherein said result document is specified in said XML notation (see Hind, col. 7, lines 19-50).

In respect to claim 6, Hind, Gennaro and Schneck disclose the computer program product according to Claim 1, wherein said stored policy enforcement objects further comprise computer-readable program code means for overriding a method for evaluating said elements of said input document, and wherein said computer-readable program code means for executing further comprises computer-readable program code means for executing said computer-readable program code means for overriding (see Hind, col. 4, lines 38-42).

In respect to claim 7, Hind, Gennaro and Schneck disclose the computer program product according to Claim 6, wherein said style sheets are specified in an Extensible Stylesheet Language (XSL) notation (see Hind, col. 4, lines 43-44).

In respect to claim 8, Hind, Gennaro and Schneck disclose the computer program product according to Claim 7, wherein said method is a value-of method of

said XSL notation, and wherein said computer-readable program code means for overriding said value-of method is by subclassing said value-of method (see Hind, col. 4, lines 43-49).

In respect to claim 9, Hind, Gennaro and Schneck disclose the computer program product according to Claim 6 or Claim 8, wherein said overridden method comprises:

computer-readable program code means for generating encryption tags (see Schneck, col. 12, lines 27-50); and computer-readable program code means for inserting said generated encryption tags into said interim transient document to surround elements of said interim transient document which are determined to require encryption; and said computer-readable program code means for encrypting selected elements encrypts those elements surrounded by said inserted encryption tags (see Schneck, Fig. 2 and 6, col. 7, lines 35-39, col. 13, lines 37-50).

In respect to claim 10, Hind, Gennaro and Schneck disclose the computer program product according to Claim 2, wherein each of said instantiated policy enforcement objects further comprises:

a specification of a community that is authorized to view said elements associated with said security policy, said specification of said communities further comprising specification of at least one of (1) one or more individual users or processes which are community members, and (2) one or more groups which are community members, wherein each of said groups comprises one or more individual users or

processes; and an encryption requirement for said elements associated with said security policy (see Schneck, col. 23, line 56-col. 24, line 4).

In respect to claim 11, Hind, Gennaro and Schneck disclose the computer program product according to Claim 10, wherein said encryption requirement further comprises specification of an encryption algorithm (see Schneck, col. 12, lines 17-26).

In respect to claim 12, Hind, Gennaro and Schneck disclose the computer program product according to Claim 10, wherein said encryption requirement further comprises specification of an encryption algorithm strength value (see Schneck, col. 12, lines 27-41).

In respect to claim 14, Hind, Gennaro and Schneck disclose the computer program product according to Claim 10, wherein said encryption requirement may have a null value to indicate that said specified security policy does not require encryption (see Schneck, Fig. 2, col. 7, lines 35-40).

In respect to claim 15, Hind, Gennaro and Schneck disclose the computer program product according to Claim 1, wherein said computer-readable program code means for encrypting selected elements uses a cipher block chaining mode encryption process (see Gennaro, col. 1, lines 19-25).

In respect to claim 19, Hind, Gennaro and Schneck disclose the computer program product according to Claim 1, wherein said DTD is replaced by a schema (see col. 8, lines 8-20, "an XML schema specifies constraints on the structures and types of elements in an xml document. The basic schema for xml is DTD").

In respect to claim 20, Hind, Gennaro and Schneck discloses the computer program product according to Claim 10, wherein said encryption requirement further comprises specification of an encryption key length (see Gennaro, col. 30, lines 41-51, maximum key length).

In respect to claim 21, Hind, Gennaro and Schneck disclose the computer program product according to Claim 9, wherein said inserted encryption tags may surround either values of said elements or values and tags of said elements (see Schneck, Fig. 2 and 6, col. 13, lines 37-50).

In respect to claim 22, the claim limitation is a system claim which is substantially similar to the computer program product of claim 1 and therefore the same rejection applied.

In respect to claim 43, the claim limitation is a method claim which is substantially similar to the computer program product of claim 1 and therefore the same rejection applied.

In respect to claims 23-33, 35-36 and 40-42, the claim limitation is a system claim which is substantially similar to the computer program product claims 2-12, 14-15, 19-21 and therefore the same rejection applied.

In respect to claims 44-54, 56-57 and 61-63, the claim limitation is a method claim which is substantially similar to the computer program product claims 2-12, 14-15 and 19-21 and therefore the same rejection applied.

5. Claim 13, 16-18, 34, 37-39, 55 and 58-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. (U.S. Patent No. 6,585,778 hereinafter Hind) in view of Gennaro et al. (U.S. Patent No. 5,937,066 hereinafter Gennaro) and Schneck et al. (U.S. Patent No. 5,933,498) and further in view of Carter (U.S. Patent No. 5,787,175).

In respect to claim 13, Hind, Gennaro and Schneck disclose the computer program product according to Claim 10, wherein said computer-readable program code means for encrypting said encryption keys further comprises:

computer-readable program code means for ensuring that said key recovery agent is one of said members of each of said communities, thereby ensuring that one of said different versions is encrypted using said public key of said key recovery agent (see Gennaro, col. 9, lines 10-15 and col. 9,line 65-col. 10, line 10).

Hind, Gennaro and Schneck do not disclose but Carter discloses a computer-readable program code means for encrypting a different version of each of said encryption keys for each of said one or more members of each of zero or more of said communities which uses said encryption key, and wherein each of said different versions is encrypted using a public key of said community member for which said different version was encrypted members (see col. 1, lines 5-14 and col. 8, lines 51-60 and col. 13, lines 63-67).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Hind, Gennaro and Schneck by creating key class for encrypted elements with associating different keys with different

users authorized to access an encrypted document to prevent redistribution of new keys when a member of a group leave the group (see Carter, col. 5, lines 5-20).

In respect to claim 16, Hind, Gennaro, Schneck and Carter disclose the computer program product according to Claim 13 further disclose said computer program product comprising:

computer-readable program code means for creating a key class comprises:

a strongest encryption requirement of associated encrypted element (see Schneck, col. 12, lines 27-65);

generating said one or more random encryption keys generates a particular one of said random encryption keys for each of said key classes (see Gennaro, col. 8, lines 55-67); and

each of said different versions in a particular key class is encrypted from said generated encryption key generated for said key class (see Gennaro, col. 8, lines 55-67); and

encrypting selected elements uses that one of said particular random encryption keys which was generated for said key class with which said selected element is associated (see col. Schneck, col. 7, lines 35-45).

for each unique community, wherein said key class is associated with each of said encrypted elements for which this unique community is an authorized viewer (see Carter, col. 1, lines 1-14);

an identifier of each of said members of said unique community (see Carter, col. 8, lines 51-60);

and one of said different versions of said encrypted encryption key for each of said identified community members (see Carter, col. 1, lines 5-14 and col. 8, lines 51-60).

In respect to claim 17, Hind, Gennaro, Schneck and disclose the computer program product according to Claim 13, wherein said computer-readable program code means for decrypting said requested output document further comprises:

computer-readable program code means for decrypting, for each of said communities said different version of said random encryption key which was encrypted using said public key of said communities (see Carter, col. 1, lines 5-14 and col. 13, lines 62-67).

wherein said computer-readable program code means for

decrypting uses a private key of said key recovery agent, thereby creating a decrypted key for each of said communities (see Gennaro, col. 9, lines 55-65 and col. 10, lines 1-35); and

computer-readable program code means for decrypting each of said encrypted

elements in said requested output document using said decrypted keys (see Gennaro, col. 10, lines 51-65); and

said computer-readable program code means for rendering further comprises:

computer-readable program code means for rendering said decrypted elements and said other unencrypted elements (see Schneck, col. 18, lines 44-61).

In respect to claim 18, Hind, Gennaro, Schneck and Carter disclose the computer program product according to Claim 16, wherein said computer-readable program code means for decrypting said requested output document further comprises:

computer-readable program code means for decrypting, for each of said key classes, said different version of said random encryption key in said key class which was encrypted using said public key of said key recovery agent, wherein said computer-readable program code means for decrypting uses a private key of said key recovery agent which is associated with said public key which was used for encryption, thereby creating a decrypted key; and computer-readable program code means for decrypting each of said encrypted elements in said requested output document using said decrypted keys (see Gennaro, col. 9, lines 10-38, col. 9, line 55-col. 10, line 27); and said computer-readable program code means for rendering further comprises:

computer-readable program code means for rendering said decrypted elements and said other unencrypted elements (see Schneck, col. 18, lines 44-61).

In respect to claims 34 and 37-39, the claim limitation is a system claim which is substantially similar to the computer program product claims 13 and 16-18 and therefore the same rejection applied.

In respect to claims 55 and 58-60, the claim limitation is a method claim which is substantially similar to the computer program product claims 13 and 16-18 and therefore the same rejection applied.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Hind et al. Disclose a retrieval of style sheets from directories based upon partial characteristic matching.

-Ciacelli et al. Disclose an apparatus, method and computer program product for protecting copyright data within a computer system.

-Kuroda discloses a security level control apparatus and method for a network securing communications between parties without presetting the security level.

-Moshfeghi discloses a method and apparatus for controlling browser functionality in the context of an application.

-Chen et al. Disclose a dynamic business process automation system using XML documents.

-Pebley et al. Disclose a system and method for transferring encrypted sections of documents across a computer network.

-Kramer et al. Discloses a hierarchical model of consumer attributes for targeting content in a privacy-reserving manner.

-Hyman et al. Disclose extension of parsable structures.

-Bailey et al. Disclose method for versioning a UML model in a repository in accordance with an updated XML representation of the UML model.

-Roberts et al. Discloses a method for creating network services by transforming an XML runtime model in response to an iterative input process.

-Livingston et al. disclose a system for presenting and managing enterprise architectures.

-Danieli discloses a security services and policy enforcement for electronic data.

Gutowitz discloses a method and apparatus for encryption decryption and authentication using dynamical systems.

-Kluttz et al. Disclose a methods, systems and computer program products for multi-level encryption.

Rucklidge et al. disclose a methods and apparatus for partial encryption of tokenized documents.

-Boag et al. Disclose a dynamically determining the most appropriate location for style sheet application.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-9600.

Examiner Tongoc Tran

Art Unit: 2134

TT
December 11, 2003

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2134